Plan d'action 2018-2020 sur les infrastructures essentielles

du Forum national intersectoriel

BÂTIR UN **CANADA SÉCURITAIRE** ET **RÉSILIENT**

Sécurité publique Canada
Public Safety Canada

Canada

© Sa Majesté la Reine du Chef du Canada, 2018

No de cat. : PS4-66/2018F-PDF
ISBN : 978-0-660-26493-6

Table des matières

1 Présentation

3 Réalisations 2010-2017

5 Le paysage des risques : Ce qui a changé

7 Mobilisation communautaire : Comment travailler ensemble

8 Mesures de suivi 2018-2020

8 Établissement de partenariats

11 Échange et protection des renseignements

13 Mise en œuvre d'une approche de gestion tous risques

17 Conclusion

18 Annexes

18 A: Rôles et responsabilités

19 B: Secteurs des infrastructures essentielles et ministères ou organismes fédéraux responsables

20 C: Réseaux sectoriels et Forum national intersectoriel

21 D: Réalisations dans le cadre du *Plan d'action sur les infrastructures essentielles* (2014-2017)

23 E: *Plan d'action 2018-2020* : Tableau sommaire

24 F: Ressources

Présentation

La sécurité nationale et la stabilité économique du Canada dépendent de la résilience des infrastructures essentielles comme les banques, les communications et les transports. Chaque jour, les Canadiens comptent sur les infrastructures essentielles pour qu'elles leur procurent des aliments salubres, de l'eau propre, un réseau électrique fiable et d'autres services essentiels.

La résilience des infrastructures essentielles du Canada dépend de la capacité des propriétaires et exploitants à réagir à un paysage des risques qui évolue à un rythme effréné. Ces risques liés, par exemple, au terrorisme, aux désastres naturels et aux cyberattaques, peuvent compromettre la sûreté et la sécurité des communautés et des infrastructures essentielles et, par extension, avoir des répercussions importantes sur le bien-être des Canadiens. Pour faire face à cet environnement de risques en constante évolution, le *Plan d'action sur les infrastructures essentielles du Forum national intersectoriel (2018-2020)* (le Plan d'action) définit des initiatives concrètes qui encouragent une approche collaborative au sein du gouvernement et du secteur des infrastructures essentielles afin d'identifier et de gérer les risques avant qu'ils n'entraînent des perturbations.

Le Plan d'action est un plan détaillé pour mettre en œuvre la *Stratégie nationale sur les infrastructures essentielles* du Canada (la Stratégie nationale). Approuvée par les ministres fédéral, provinciaux et territoriaux responsables de la gestion des urgences en 2010, la Stratégie nationale définit ce qu'on entend par infrastructures essentielles, soit l'ensemble des processus, des systèmes, des installations, des technologies, des réseaux, des biens et des services nécessaires pour assurer la santé, la sûreté, la sécurité ou le bien-être économique des Canadiens ainsi que l'efficacité du gouvernement.

La Stratégie nationale est fondée sur les principes énumérés dans le *Cadre de sécurité civile pour le Canada* qui reconnaît le rôle que doivent jouer divers intervenants dans le système national de gestion des urgences afin d'améliorer la sécurité des Canadiens. De même, la Stratégie nationale souligne le fait que les responsabilités en matière de protection des infrastructures essentielles au Canada sont partagées entre les gouvernements fédéral, provinciaux et territoriaux, les autorités locales et les propriétaires et exploitants de ces infrastructures essentielles. Ces derniers sont par ailleurs les principaux responsables de la protection de leurs biens et services. La relation est mutuellement bénéfique : la Stratégie nationale reconnaît que les propriétaires et exploitants des infrastructures essentielles détiennent l'expertise et l'information dont les gouvernements ont besoin pour élaborer des plans et des politiques utiles et mettre en œuvre des programmes et des initiatives efficaces. En retour, les gouvernements jouent un rôle clé en fournissant de l'information à propos des risques pertinents pour les propriétaires et exploitants afin de les aider dans le cadre de leurs activités de gestion des risques.

En plus de la Stratégie nationale, le premier *Plan d'action sur les infrastructures essentielles (2010-2013)* ciblait des domaines de collaboration pour les gouvernements fédéral, provinciaux et territoriaux, ainsi que les propriétaires et exploitants d'infrastructures essentielles. Il établissait aussi un réseau intersectoriel national pour chacun des dix secteurs d'infrastructures

essentielles, et un ministère ou organisme fédéral a été principalement chargé de chacun de ces réseaux (voir l'annexe B). En outre, la Stratégie nationale a mis sur pied le Forum national intersectoriel (FNI) pour encourager la collaboration entre les réseaux sectoriels. Le FNI est une entité de consultation et de sensibilisation d'envergure nationale qui réunit des dirigeants des 10 secteurs des infrastructures essentielles du Canada dans le but d'identifier des priorités et de discuter d'enjeux pertinents pour les divers secteurs, ainsi que d'initiatives pour accroître la résilience des biens et systèmes vitaux du Canada (voir l'annexe C).

Avec le deuxième *Plan d'action sur les infrastructures essentielles (2014-2017)*, des progrès ont été réalisés pour renforcer les infrastructures essentielles et les rendre plus résilientes. Par exemple, le Programme d'évaluation de la résilience régionale (PERR) de Sécurité publique Canada a été mis en œuvre à travers le Canada et étendu pour inclure un outil d'évaluation de la cybersécurité. En même temps, on a procédé à des exercices et des réunions de réseaux multisectoriels ont eu lieu pour identifier les interdépendances et aborder les enjeux qui concernent plusieurs secteurs.

Le Plan d'action 2018-2020 continue de soutenir les trois objectifs stratégiques identifiés dans la Stratégie nationale afin de renforcer la résilience des infrastructures essentielles au Canada :

- établissement de partenariats;
- échange et protection de l'information;
- mise en œuvre d'une approche de gestion tous risques.

Cette réitération du Plan d'action prévoit des activités concrètes pour chacun des trois objectifs stratégiques et examine de plus près les risques auxquels la communauté des infrastructures essentielles est confrontée aujourd'hui, et ceux auxquels elle pourrait être confrontée au cours des prochaines années. Elle tient également compte des réalisations découlant des efforts collaboratifs passés et en cours au sein de tous les ordres de gouvernement et du secteur des infrastructures essentielles.

Réalisations 2010-2017

Depuis la publication de la Stratégie nationale, les gouvernements (fédéral, provinciaux et territoriaux), ainsi que le secteur privé, ont travaillé ensemble pour réaliser d'énormes progrès en matière d'amélioration et de maintien des partenariats. Plus précisément, depuis 2010, Sécurité publique Canada, de pair avec les principaux ministères et organismes fédéraux, a établi des réseaux intersectoriels qui se rencontrent régulièrement, a mis sur pied des rencontres annuelles du *Forum national intersectoriel* et a organisé des réunions multisectorielles fort courues pour parler des enjeux qui concernent les dix secteurs des infrastructures essentielles. En outre, au cours des dernières années, Sécurité publique Canada a travaillé en étroite collaboration avec les provinces et les territoires pour renforcer les partenariats entre les gouvernements.

Pour ce qui est de l'échange et de la protection de l'information, depuis le dernier Plan d'action, Sécurité publique Canada a doublé le nombre de membres de la Passerelle d'information canadienne sur les infrastructures essentielles (Passerelle IE), tout en continuant à fournir des renseignements sur les risques à la communauté canadienne des infrastructures essentielles, et ce, tant en période de régime stable que lors d'incidents perturbateurs. Des mesures ont aussi été prises pour garantir que les membres de la communauté des infrastructures essentielles ont accès à des renseignements utiles en temps opportun, ce qui inclut, entre autres, de faciliter l'obtention d'attestations de sécurité pour les membres du FNI. En outre, la collectivité continue de chercher activement à diffuser de l'information sur la cybersécurité dans le but de protéger les entreprises et les consommateurs du Canada, notamment dans le cadre de l'Échange canadien de renseignements sur les menaces cybernétiques (ECMC), une organisation indépendante à but non lucratif dont la mission est de diffuser de l'information sur les menaces, de mener des analyses des cybermenaces et de recommander des mesures d'atténuation des risques.

Sécurité publique Canada a aussi travaillé en étroite collaboration avec tous les ordres de gouvernement et les partenaires du secteur privé sur plusieurs aspects afin de concevoir des activités de gestion des risques dans une perspective tous risques. Par exemple, des efforts accrus dans le cadre du PERR ont permis aux hauts fonctionnaires du Ministère de travailler directement avec les propriétaires et exploitants des dix secteurs des infrastructures essentielles afin d'identifier et d'atténuer les vulnérabilités de leurs établissements. Travaillant en étroite collaboration avec la communauté des infrastructures essentielles et des alliés internationaux, Sécurité publique Canada a aussi renforcé le rôle de base de la Cellule pour l'analyse virtuelle des risques (CAVR) qui procure l'expertise et l'analyse pour identifier les impacts possibles des incidents perturbateurs et soutient une meilleure planification, de même qu'une intervention et un rétablissement plus rapides lorsque ces événements surviennent. Sécurité publique Canada a également organisé plusieurs exercices qui ont permis de réunir des communautés d'experts et de tirer profit des leçons apprises et y a participé. Finalement, le Ministère a continué à offrir et à étendre sa formation sur la cybersécurité des systèmes de contrôle industriels (SCI) et ses événements pour favoriser l'esprit communautaire afin de contribuer à bâtir une expertise et une capacité en cybersécurité au sein des secteurs des infrastructures essentielles du Canada.

Aussi, dans le cadre des efforts continus pour offrir aux secteurs des infrastructures essentielles des outils et de l'information pour gérer les principaux risques, un groupe de travail dirigé par l'industrie a développé, dans le cadre du FNI, les *Principes fondamentaux de cybersécurité à l'intention du milieu des infrastructures essentielles du Canada*. Ce document, qui appuie et fait la promotion de l'adoption du cadre de cybersécurité du *National Institute of Standards and Technology*, donne des orientations axées sur l'action afin d'aider les organisations à atteindre un niveau de base en cybersécurité.

Finalement, reconnaissant le fait que les infrastructures essentielles sont interreliées, non seulement à travers le Canada, mais aussi à travers le monde, Sécurité publique Canada a cherché à faire la promotion d'une approche coordonnée et globale en matière d'infrastructures essentielles. Par exemple, le Canada et les États-Unis ont déployé beaucoup d'efforts pour atteindre des objectifs communs d'amélioration de la résilience des infrastructures essentielles présentant un intérêt mutuel, et ce, en travaillant dans les différents secteurs et ressorts. Le Canada a également travaillé en étroite collaboration avec la communauté internationale, y compris nos partenaires du Groupe des cinq (États-Unis, Royaume-Uni, Australie, Nouvelle-Zélande), afin de garantir que son approche pour renforcer la résilience des infrastructures essentielles tient compte du contexte global et tire profit des meilleures pratiques des alliés dignes de confiance.

Un résumé des activités complétées dans le cadre du *Plan d'action sur les infrastructures essentielles (2014-2017)* est disponible à l'annexe D.

Le paysage des risques:
Ce qui a changé

Le Plan d'action 2018-2020 est fondé sur une approche tous risques tenant compte du nouvel environnement des risques, des vulnérabilités connues et des stratégies d'atténuation possibles. L'environnement de risques continuera forcément d'évoluer, et l'approche du Canada devra être modifiée et adaptée en conséquence.

Les effets des changements climatiques au Canada continuent d'être un des principaux risques qui ont des répercussions directes sur les infrastructures essentielles. Les modèles des changements climatiques suggèrent des fluctuations des précipitations, du niveau de la mer, du niveau des eaux intérieures et du pergélisol, ainsi qu'une plus grande fréquence de conditions météorologiques extrêmes. Les phénomènes météorologiques violents peuvent avoir des répercussions importantes sur les infrastructures, ce qui peut non seulement nécessiter la mobilisation d'importantes ressources supplémentaires pour les interventions et le rétablissement, mais également entraîner des conséquences dévastatrices qui se répercutent en cascade sur la chaîne d'approvisionnement. L'élaboration de stratégies d'adaptation pour les infrastructures dans les régions exposées à des phénomènes météorologiques extrêmes plus fréquents sera essentielle pour réduire les impacts sociaux et économiques des changements climatiques.

La convergence croissante des domaines virtuel et physique présente également de nouveaux défis pour les infrastructures essentielles du Canada. L'augmentation du recours aux services publics connectés, à l'automatisation et à l'intelligence artificielle, de même que la multiplication des appareils branchés, offre d'énormes possibilités aux secteurs des infrastructures essentielles et à l'économie canadienne puisque les technologies permettent des analyses plus rapides et contribuent à faire fonctionner les systèmes de façon plus efficace. Les services publics connectés intègrent les cybertechnologies et l'infrastructure physique pour améliorer l'efficacité des centres urbains au plan environnemental et économique, de même que la mobilité des personnes et des biens (p. ex. des réseaux électriques interconnectés pour réduire les pertes, des systèmes de transport plus intelligents et mieux synchronisés). Cependant, le fait que les organisations se fient de plus en plus aux cybersystèmes et aux technologies entraîne une exposition à de nouveaux risques qui pourraient avoir d'importantes conséquences physiques. Les systèmes SCI se situent à la frontière de la cybersécurité et de la sécurité physique. Ces systèmes, dont plusieurs ont été développés avant l'avènement de l'ère Internet, sont utilisés pour un éventail d'applications cruciales, y compris dans les secteurs de l'énergie et des services publics, du transport, de la santé, de la fabrication, des aliments et de l'eau potable. Pour diverses raisons, y compris les efforts pour réduire les coûts et améliorer l'efficience, ces systèmes sont de plus en plus connectés à Internet, ce qui peut entraîner l'exposition à des menaces plus complexes que celles prises en compte au moment de leur conception.

Une autre menace complexe et en évolution pour les infrastructures essentielles du Canada est le terrorisme. Le gouvernement du Canada continue d'adapter son approche globale pour

protéger les Canadiens à la suite de la publication de *Renforcer la résilience face au terrorisme : Stratégie antiterroriste du Canada* (2012). La Stratégie antiterroriste met en évidence l'importance de la coopération avec les partenaires internationaux du Canada, tous les ordres de gouvernement, les organismes du renseignement et d'application de la loi, les intervenants de l'industrie et la société civile. Le gouvernement du Canada a aussi publié le *Rapport public de 2017 sur la menace terroriste pour le Canada*, lequel fournit d'autres détails sur les tendances en matière de terrorisme et ce qu'elles signifient pour les Canadiens. À cette fin, Sécurité publique Canada continue de travailler en étroite collaboration avec des intervenants importants des infrastructures essentielles, les gouvernements et les organismes de sécurité et du renseignement [c.-à-d. la Gendarmerie royale du Canada (GRC), le Service canadien du renseignement de sécurité (SCRS), l'Agence des services frontaliers du Canada (ASFC) et le Centre canadien de réponse aux incidents cybernétiques (CCRIC)] afin d'évaluer le contexte de menaces changeant et d'offrir de l'information pertinente à la communauté des infrastructures essentielles.

Finalement, les infrastructures vieillissantes posent aussi de plus en plus un risque. Plusieurs infrastructures approchent, ou ont dépassé, la fin de leur vie utile, ce qui peut entraîner des coûts d'entretien à la hausse et un risque accru de perturbation. Identifier les stratégies de réduction des risques liés aux infrastructures vieillissantes sera essentiel pour réduire les répercussions importantes possibles en cas de défaillance sur la sécurité nationale, notre économie et le bien-être des Canadiens.

Mobilisation communautaire :
Comment travailler ensemble

En plus de traiter des dangers et menaces actuels et émergents pour les infrastructures essentielles, le présent Plan d'action tient compte des opinions et observations reçues lors de consultations et de nombreux événements de mobilisation. En 2016, Sécurité publique Canada a tenu une consultation sur la cybersécurité afin d'examiner les mesures en place pour protéger les Canadiens et les infrastructures essentielles du Canada contre les cybermenaces. Les résultats de ces consultations ont souligné l'importance des technologies numériques pour les infrastructures essentielles, tout en reconnaissant l'émergence de nouvelles vulnérabilités.

Plus récemment, Sécurité publique Canada a consulté le gouvernement fédéral, les provinces et les territoires, ainsi que les propriétaires et exploitants d'infrastructures essentielles pour connaître leur opinion sur les mécanismes de partage d'information et sur les principaux programmes de renforcement de la résilience, dont le Programme d'évaluation de la résilience régionale (PERR) et la Cellule pour l'analyse virtuelle des risques (CAVR). Sécurité publique Canada a également consulté les groupes d'intérêts liés aux infrastructures essentielles par diverses autres initiatives de mobilisation, comme des réunions de réseaux sectoriels et d'autres événements communautaires. Les opinions et observations obtenues des dix secteurs grâce à ces divers événements ont permis d'éclairer l'élaboration du présent Plan d'action.

En vertu du Plan d'action 2014-2017, Sécurité publique Canada a renouvelé l'accent mis sur la collaboration au moyen du Groupe de travail fédéral-provincial-territorial sur les infrastructures essentielles. À l'avenir, cette démarche renouvelée permettra à tous les paliers de gouvernement de travailler ensemble en complémentarité pour atteindre des objectifs communs de résilience des infrastructures essentielles. Elle permettra également à la communauté des infrastructures essentielles de soutenir efficacement les mécanismes de gouvernance intergouvernementaux (comme les cadres supérieurs fédéraux, provinciaux et territoriaux responsables de la gestion des urgences et les ministres fédéraux, provinciaux et territoriaux responsables de la gestion des urgences), tout en venant complémenter l'action des forums permanents de mobilisation publics-privés, comme les réseaux sectoriels, les réseaux multisectoriels et le Forum national intersectoriel.

Mesures de suivi 2018-2020

Le présent Plan d'action soutient les principes de gestion des risques définis dans la Stratégie nationale. La section ci-dessous définit les mesures de suivi pour chacun des objectifs stratégiques de la Stratégie nationale, qui s'appuient sur les réalisations passées et les leçons tirées. Ces activités visent à renforcer la résilience des infrastructures essentielles du Canada par des activités de prévention, d'atténuation, de préparation, d'intervention et de rétablissement en cas de perturbation. Elles visent à favoriser la collaboration et l'échange de renseignements entre tous les paliers de gouvernement et les partenaires du secteur privé, en se concentrant sur l'exécution d'initiatives tangibles de gestion des risques. Un tableau résumant les mesures à prendre et les échéanciers de mise en œuvre connexes se trouve à l'annexe E.

ÉTABLISSEMENT DE PARTENARIATS

Renforcer la résilience des infrastructures essentielles requiert un travail de collaboration par tous les partenaires et toutes les parties prenantes. Sécurité publique Canada travaille en étroite collaboration avec les ministères et organismes fédéraux, les provinces et les territoires, le secteur privé et des homologues étrangers pour construire des partenariats et promouvoir des objectifs communs. Les mesures de suivi ci-dessous sont axées sur l'établissement, le maintien et l'amélioration de la collaboration avec tous les partenaires du milieu des infrastructures essentielles. Elles visent également à créer ou à entretenir des structures et mécanismes pour faciliter la coopération et l'échange de renseignements.

1. Tenir compte des problèmes dans l'ensemble des secteurs lors de réunions multisectorielles.

Les réunions multisectorielles se sont révélées un moyen efficace de tenir compte des problèmes dans l'ensemble des secteurs. La participation des hauts dirigeants des dix secteurs des infrastructures essentielles est assurée par l'entremise du Forum national intersectoriel sur les infrastructures essentielles, coprésidé par le sous-ministre de Sécurité publique Canada (SP), et soutenu par des discussions de niveau opérationnel aux réunions du Réseau multisectoriel (RMS). Outre le Forum national intersectoriel et le Réseau multisectoriel, Sécurité publique Canada assumera la responsabilité de la coordination des réunions intersectorielles spéciales afin de tenir compte des problèmes d'intérêt commun.

Résultats attendus

1.1 Les membres du Forum national intersectoriel se rencontreront en personne et participeront à des téléconférences spéciales. Sécurité publique Canada coordonnera et organisera toutes les rencontres.
Calendrier : en continu

1.2 Réunion annuelle en personne du RMS. Sécurité publique Canada assumera la responsabilité de la coordination des réunions multisectorielles spéciales supplémentaires.
Calendrier : en continu

2. Collaborer avec les provinces et les territoires afin de renforcer la résilience des infrastructures essentielles

Sécurité publique Canada continuera de collaborer avec d'autres paliers de gouvernement, principalement par l'entremise du Groupe de travail fédéral-provincial-territorial sur les infrastructures essentielles, collaborant sur les problèmes actuels et émergents des secteurs des infrastructures essentielles, notamment en ce qui a trait aux relations avec la gestion des urgences, la sécurité nationale et la cybersécurité. Sécurité publique Canada et les provinces et territoires travailleront de concert pour cerner les occasions pour les provinces et territoires de profiter des programmes fédéraux relatifs aux infrastructures essentielles, comme le Programme d'évaluation de la résilience régionale (PERR), pour soutenir les efforts locaux de renforcement de la résilience.

Résultats attendus

2.1 Sécurité publique Canada coordonnera et présidera les réunions du Groupe de travail fédéral-provincial-territorial sur les infrastructures essentielles.
Calendrier : en continu

2.2 Le Groupe de travail fédéral-provincial-territorial sur les infrastructures essentielles élaborera et mettra en œuvre un Plan de travail pour définir et orienter ses activités.
Calendrier : en continu

2.3 Sécurité publique Canada travaillera avec les provinces et territoires afin de déterminer des moyens de collaborer plus efficacement à l'exécution des programmes relatifs aux infrastructures essentielles, notamment le PERR.
Calendrier : 1re année

3. Collaborer de manière continue avec les ministères fédéraux responsables

Sécurité publique Canada continuera de fournir une direction et un soutien à la communauté fédérale des infrastructures essentielles, y compris assurer un rôle de coordination pour ce qui est du Réseau des ministères fédéraux responsables des infrastructures essentielles. Ce Réseau rassemble des ministères et organismes fédéraux responsables des dix secteurs d'infrastructures essentielles afin de soutenir l'échange de renseignements et la collaboration. De plus, Sécurité publique Canada prévoit mettre sur pied une communauté d'experts fédéraux en cybersécurité issus de ces dix secteurs afin de s'attaquer aux risques de cybersécurité associés aux infrastructures essentielles. Sécurité publique Canada continuera de collaborer étroitement avec les autres organismes gouvernementaux et les bureaux régionaux.

Résultats attendus

3.1 Les membres du Réseau des ministères fédéraux responsables des infrastructures essentielles se réuniront régulièrement à l'échelon des directeurs. Sécurité publique Canada présidera et coordonnera les réunions.
Calendrier : en continu

3.2 Sécurité publique Canada travaillera avec les ministères fédéraux responsables pour renforcer les partenariats dans le domaine de la cybersécurité en dirigeant la création d'une communauté d'experts de la cybersécurité des infrastructures essentielles.
Calendrier : 1re année et en continu

4. Accroître la portée régionale des programmes des infrastructures essentielles

Pour améliorer le rayonnement et l'impact des programmes de Sécurité publique Canada, le Ministère élaborera une stratégie de rayonnement pour les principaux programmes d'amélioration de la résilience. Pour atteindre cet objectif, des partenariats seront établis avec d'autres paliers de gouvernement, des communautés autochtones, des propriétaires ou exploitants d'infrastructures essentielles, les milieux universitaires, ainsi que des partenaires du gouvernement fédéral et de l'étranger.

Résultats attendus

4.1 Sécurité publique Canada élaborera et mettra en œuvre une stratégie de rayonnement pour les principaux programmes d'amélioration de la résilience
Calendrier : 1re année

5. Participer à différents forums internationaux pour aborder les questions touchant les infrastructures essentielles

Sécurité publique Canada continuera de participer à divers groupes internationaux, comme le Groupe des cinq. Ces groupes ont été mis sur pied afin de fournir une tribune pour discuter des questions d'intérêt mutuel portant sur la résilience des infrastructures essentielles.

Résultats attendus

5.1 Sécurité publique Canada dirigera la participation du Canada aux groupes internationaux afin de promouvoir une approche axée sur la collaboration visant à renforcer la résilience des biens et des systèmes interreliés à l'échelle mondiale et à communiquer les pratiques exemplaires.
Calendrier : en continu

ÉCHANGE ET PROTECTION DES RENSEIGNEMENTS

L'échange et la protection des renseignements sont indispensables pour renforcer la résilience des infrastructures essentielles. L'échange de renseignements en temps opportun entre les gouvernements et les secteurs d'infrastructures essentielles est nécessaire pour promouvoir la gestion efficace des risques. Les mesures de suivi décrites ci-dessous ont pour but d'aider à veiller à ce que les intéressés aient accès aux bons renseignements au bon moment pour soutenir la planification et le processus décisionnel, tant en période de stabilité qu'au moment d'incidents perturbateurs. Ces initiatives supposent une démarche en collaboration afin d'évaluer le type de renseignements produits, les personnes avec qui ils sont échangés et la façon dont ils le sont.

6. Moderniser et promouvoir la Passerelle d'information sur les infrastructures essentielles

Sécurité publique Canada s'affairera à moderniser la Passerelle d'information sur les infrastructures essentielles afin d'améliorer sa fonctionnalité et l'expérience des utilisateurs. Cette initiative de modernisation comprendra également un examen des publications et des outils existants pour s'assurer qu'ils demeurent pertinents. En outre, Sécurité publique Canada mettra l'accent sur l'augmentation du nombre d'utilisateurs de la Passerelle, plus particulièrement en ciblant les régions et les secteurs où un plus faible taux de participation est observé.

Résultats attendus

6.1 Sécurité publique Canada modernisera la Passerelle d'information sur les infrastructures essentielles pour mettre à jour les renseignements et améliorer l'expérience des utilisateurs.
Calendrier : 1re année

6.2 Sécurité publique Canada fera activement la promotion de l'utilisation de la Passerelle d'information sur les infrastructures essentielles pour inclure une plus grande représentation régionale et sectorielle.
Calendrier : 1re année et en continu

7. Procéder à une analyse environnementale sur l'échange de renseignements

En s'appuyant sur le cadre d'échange de renseignements sur les infrastructures essentielles, Sécurité publique Canada effectuera une analyse environnementale pour cerner les lacunes des mécanismes d'échange de renseignements existants. Cette initiative explorera également ces mécanismes pour améliorer les modalités de diffusion des renseignements afin d'en assurer la rapidité et l'accessibilité pour le milieu des infrastructures essentielles. Une partie de l'objectif consiste à évaluer les protocoles sur l'échange de renseignements en cas d'incident, c'est-à-dire : quoi, quand, avec qui et de quelle manière.

Résultats attendus

7.1 Examiner le cadre d'échange des renseignements sur les infrastructures essentielles existant, effectuer une analyse environnementale des mécanismes d'échange de renseignements en place et en cerner les lacunes potentielles.
Calendrier : 2e année

7.2 Cerner les obstacles et examiner les mécanismes afin d'améliorer l'échange de renseignements entre le gouvernement fédéral, les provinces et les territoires, ainsi que les propriétaires et les exploitants.
Calendrier : 2e année

8. Élaborer et diffuser les renseignements en période de stabilité et au moment d'incidents perturbateurs

Sécurité publique Canada, par l'entremise de la Cellule pour l'analyse virtuelle des risques (CAVR), fournit des renseignements au gouvernement et aux partenaires du secteur privé en période de régime stable et au cours d'événements en cours. La CAVR continuera de fournir des renseignements sur les risques, notamment les évaluations des risques et des répercussions, les renseignements pertinents sur la continuité des activités et la gestion des urgences, l'analyse des liens de dépendance et d'interdépendance qui caractérisent les infrastructures essentielles, les produits géospatiaux, la modélisation de la chaîne d'approvisionnement, ainsi que les données statistiques pertinentes. En continuant d'élaborer ces types de produits, et en étant guidée par les pratiques de l'industrie comme l'Échange canadien de renseignements sur les menaces cybernétiques (ECMC), Sécurité publique Canada appuiera les efforts de gestion des risques des intervenants des infrastructures essentielles.

Résultats attendus

8.1 Sécurité publique Canada élaborera et échangera des données d'analyse et des produits d'information afin de soutenir la gestion des risques touchant les infrastructures essentielles par les intervenants.
Calendrier : en continu

8.2 Sécurité publique Canada fera la promotion des outils de modélisation afin de soutenir l'analyse des liens de dépendance et d'interdépendance.
Calendrier : en continu

9. Appuyer l'obtention d'attestations de sécurité parmi les intervenants du secteur privé

Sécurité publique Canada collaborera avec les ministères fédéraux responsables afin d'accroître le nombre d'intervenants ayant obtenu une cote de sécurité de niveau « secret ». Cette initiative garantira l'échange de renseignements jugés sensibles avec les personnes compétentes.

Résultats attendus

9.1 Les ministères fédéraux responsables et Sécurité publique Canada travailleront ensemble à cerner des moyens d'accroître l'accès aux attestations de sécurité pour les secteurs des infrastructures essentielles et exploreront des mécanismes pour rationaliser le processus d'obtention (p. ex. les délais d'obtention, la transférabilité des attestations de sécurité).
Calendrier : en continu

9.2 Sécurité publique Canada travaillera avec les ministères fédéraux responsables et les partenaires du portefeuille pour promouvoir l'utilisation de renseignements déclassifiés, ou partiellement déclassifiés, pour soutenir la conscience situationnelle.
Calendrier : 1re année et en continu

MISE EN ŒUVRE D'UNE APPROCHE DE GESTION TOUS RISQUES

La Stratégie nationale fait la promotion de la gestion du risque et d'une solide planification de la continuité des activités afin de renforcer la résilience des infrastructures essentielles. En adoptant une démarche fondée sur le risque, les gouvernements et le secteur privé peuvent évaluer la probabilité et les conséquences d'une perturbation potentielle et allouer des ressources en fonction de leur tolérance au risque. Les évaluations de risque peuvent aider à développer une solide conscience situationnelle des défis présentés par la convergence des dangers, des menaces et des vulnérabilités touchant les infrastructures essentielles au Canada. Dans ce contexte, Sécurité publique Canada et les ministères et organismes fédéraux responsables travaillent en étroite collaboration avec les provinces et territoires ainsi qu'avec les intéressés en matière d'infrastructures essentielles pour mieux comprendre ces risques. Les éléments ci-dessous ont pour objectif de contribuer à veiller à ce que le milieu des infrastructures essentielles dispose des outils et des renseignements nécessaires pour prendre des mesures significatives de gestion des risques dans une perspective de gestion tous risques.

10. Accroître l'impact des évaluations de résilience

Pour favoriser l'impact du programme, le PERR travaillera à établir un partenariat avec les provinces et territoires, tout en conservant un rôle directeur à l'échelle nationale. En outre, les responsables du Programme d'évaluation de la résilience régionale envisageront d'inclure d'autres modules au sein des outils d'évaluation actuels afin d'accroître la précision de l'évaluation dans des secteurs en particulier. Enfin, dans le cadre du Programme d'évaluation de la résilience régionale, les responsables de l'Examen canadien de la cyberrésilience (ECCR) continueront d'évaluer les installations partout au Canada afin de renforcer la résilience des propriétaires et des exploitants envers les cybermenaces, tout en examinant d'autres outils visant à accroître la précision des évaluations dans le cadre de l'ECCR.

Résultats attendus

10.1 Sécurité publique Canada travaillera avec les provinces et territoires à définir et à mettre en œuvre des mesures pour accroître l'impact et le rayonnement du PERR.
Calendrier : 1re année

10.2 Sécurité publique Canada continuera d'offrir l'ECCR partout au Canada et d'analyser les possibilités quant à la fourniture d'autres outils aux fins de soutien et de complément à l'ECCR.
Calendrier : 1re année

10.3 Évaluer les besoins d'évaluation et la faisabilité de l'ajout de modules aux outils d'évaluation du PERR afin d'accroître la précision de l'analyse sur des sujets en particulier.
Calendrier : 2e année

11. Mettre en œuvre une approche axée sur les risques pour cerner les biens et les infrastructures à caractère important

Sécurité publique Canada collaborera avec les ministères fédéraux responsables afin d'examiner et de mettre à jour la liste des biens d'infrastructures essentielles canadiens, et d'étudier les possibilités d'affiner davantage la méthodologie liée à la détermination des biens d'importance nationale. La liste servira, entre autres, à orienter le processus de sélection des sites dans le cadre du PERR. Le processus de sélection des sites et le plan annuel d'évaluation qui en découle s'appuieront également sur les commentaires des provinces et territoires et des ministères fédéraux responsables, et sur une évaluation objective de la criticité de chaque installation.

Résultats attendus

11.1 Sécurité publique Canada collaborera avec les ministères fédéraux responsables afin de passer en revue et de mettre à jour la liste des biens d'infrastructures essentielles
Calendrier : 1re année (et en continu)

11.2 Sécurité publique Canada établira des critères axés sur le risque pour évaluer objectivement la criticité des installations (indice d'exposition à la criticité).
Calendrier : 1re année

11.3 Sécurité publique Canada élaborera et mettra en œuvre un plan annuel d'évaluation des sites du PERR.
Calendrier : 1re année (et en continu)

12. Déterminer des moyens pour encourager la communauté des infrastructures essentielles à prendre des mesures afin de réduire les risques

Sécurité publique Canada étudiera les moyens de favoriser les mesures d'atténuation des risques après la tenue des évaluations de la résilience. L'objectif consiste à trouver des mécanismes visant à encourager les intervenants à prendre des mesures pour aborder les enjeux et les

vulnérabilités systémiques qui ont été mis en lumière. En outre, Sécurité publique Canada tentera de cerner les nouveaux risques pour les infrastructures essentielles et examinera les collaborations possibles avec des partenaires sectoriels pour mieux faire connaître les risques et les réduire.

Résultats attendus

12.1 Sécurité publique Canada collaborera avec les intervenants des infrastructures essentielles pour trouver des moyens efficaces d'aider les propriétaires et les exploitants à prendre des mesures de gestion des risques.
Calendrier : en continu

12.2 Sécurité publique Canada collaborera avec des partenaires sectoriels afin de cerner les nouveaux risques pour les infrastructures essentielles et de les faire connaître (p. ex. infrastructures vieillissantes, changements climatiques, intelligence artificielle, drones).
Calendrier : 2e année (et en continu)

13. Tenir des exercices intersectoriels visant à renforcer les activités de préparation et d'intervention

La communauté des infrastructures essentielles a ciblé des exercices comme moyen efficace de mettre à l'essai, d'évaluer et d'améliorer la planification. En appui à une approche mutuelle visant à accroître la résilience, Sécurité publique Canada continuera à tenir des exercices intersectoriels en collaboration avec les ministères fédéraux responsables, les provinces et territoires, ainsi que les propriétaires et les exploitants d'infrastructures essentielles. Afin de favoriser l'apprentissage organisationnel, Sécurité publique Canada communiquera les observations et les pratiques exemplaires tirées des exercices pour faire avancer les questions systémiques communes à la communauté des infrastructures essentielles.

Résultats attendus

13.1 Sécurité publique Canada continuera de tenir des exercices intersectoriels physiques et axés sur la cybernétique en collaboration avec les ministères fédéraux responsables, les provinces et territoires, ainsi que les propriétaires et les exploitants d'infrastructures essentielles.
Calendrier : en continu

13.2 Sécurité publique Canada communiquera les observations et les pratiques exemplaires tirées des exercices.
Calendrier : en continu

14. Évaluer l'état de santé des dix réseaux sectoriels des infrastructures essentielles

Sécurité publique Canada concevra et mettra en œuvre un processus permettant d'évaluer et d'améliorer la « santé » des réseaux sectoriels, en consultation avec les ministères fédéraux responsables et les représentants de l'industrie. Sécurité publique Canada préparera un rapport qui déterminera les forces et les domaines à améliorer au sein et à l'échelle des secteurs pour soutenir l'élaboration d'outils et de pratiques exemplaires, renforcer les partenariats, et accroître l'intérêt collectif envers les questions prioritaires.

Résultats attendus

14.1 Sécurité publique Canada collaborera avec les ministères fédéraux responsables afin d'élaborer un processus d'évaluation de la santé des réseaux sectoriels des infrastructures essentielles.
Calendrier : 1re année

14.2 Sécurité publique Canada collaborera avec les membres du Forum national intersectoriel et les ministères fédéraux responsables afin de déterminer les prochaines étapes de l'amélioration de la santé des réseaux sectoriels.
Calendrier : en continu

15. Soutenir la communauté dans la gestion des risques associés à la convergence des systèmes d'infrastructures essentielles physiques et cybernétiques

Les infrastructures essentielles du Canada dépendent de plus en plus de systèmes et de biens cybernétiques. Pour réduire les risques associés à la convergence des systèmes d'infrastructures essentielles physiques et cybernétiques, Sécurité publique Canada continuera d'offrir des séances de formation sur la protection des SCI et de réunir des intervenants pour mettre en commun leurs connaissances et leur expérience sur l'atténuation des cybermenaces. En étroite collaboration avec les ministères fédéraux responsables et les propriétaires et exploitant des infrastructures essentielles, Sécurité publique Canada étudiera les moyens d'accroître sa portée au sein des dix secteurs des infrastructures essentielles.

Résultats attendus

15.1 Sécurité publique Canada tiendra des symposiums sur la cybersécurité des SCI dans différentes villes du Canada.
Calendrier : en continu

15.2 Sécurité publique Canada collaborera étroitement avec les intervenants du milieu des infrastructures essentielles afin d'accroître la portée des mécanismes de participation en matière de cybernétique, comme les symposiums sur la sécurité des SCI.
Calendrier : 1re année

16. Réviser la *Stratégie nationale pour les infrastructures essentielles* (2010) afin de déterminer s'il y a un besoin de mettre à jour l'approche globale du Canada pour la résilience des infrastructures essentielles

La *Stratégie nationale sur les infrastructures essentielles* (la Stratégie) a été publiée en 2010, et elle continue d'orienter l'approche globale axée sur la résilience des infrastructures essentielles au Canada. Pour garantir la pertinence continue de nos efforts de résilience, Sécurité publique Canada procédera à un examen de la Stratégie afin de déterminer s'il faut la renouveler ou la mettre à jour, en collaborant étroitement avec les provinces, les territoires, la communauté fédérale et le secteur privé.

Résultats attendus

16.1 Sécurité publique Canada examinera la *Stratégie nationale sur les infrastructures essentielles*, en étroite collaboration avec les provinces, les territoires, la communauté fédérale et le secteur privé.
Calendrier : 3e année

17. Concevoir un mécanisme de suivi pour évaluer la progression des activités du Plan d'action

Sécurité publique Canada assurera un suivi des progrès des activités énoncées dans le Plan d'action. Elle apportera des rajustements aux mesures de suivi, au besoin, afin de s'assurer d'atteindre l'objectif principal. À cette fin, Sécurité publique Canada concevra un outil de suivi, lequel déterminera le résultat prévu pour chaque produit livrable, et permettra de produire régulièrement des rapports sur les progrès accomplis.

Résultats attendus

17.1 Sécurité publique Canada élaborera un mécanisme de suivi des mesures et de production de rapports réguliers sur l'atteinte des objectifs.
Calendrier : 1re année et en continu

Conclusion

La *Stratégie nationale sur les infrastructures essentielles* continuera d'orienter l'approche globale du Canada quant au renforcement des infrastructures essentielles. Ce Plan d'action actualisé propose un modèle de collaboration avec d'autres ministères et organismes fédéraux, les provinces, les territoires et les intervenants du milieu des infrastructures essentielles. Les mesures décrites pour les trois prochaines années continueront de s'inspirer des succès obtenus jusqu'à présent par les plans d'action précédents en tenant compte des leçons apprises, en améliorant constamment les produits existants et en explorant de nouvelles possibilités.

Annexe A :
Rôles et responsabilités

Acteur	Rôle	Responsabilités
Gouvernement fédéral	Diriger les activités fédérales	• Favoriser une approche fédérale, provinciale et territoriale pour améliorer la résilience des infrastructures essentielles • Collaborer avec les provinces et les territoires pour atteindre les objectifs de la Stratégie • Collaborer avec les associations nationales • Collaborer avec les propriétaires et exploitants d'infrastructures essentielles conformément au mandat fédéral, avec l'accord des provinces et des territoires
Gouvernements provinciaux et territoriaux	Diriger des activités provinciales ou territoriales	• Favoriser une approche fédérale, provinciale et territoriale pour améliorer la résilience des infrastructures essentielles • Collaborer avec le gouvernement fédéral, les provinces et les territoires pour atteindre les objectifs de la Stratégie • Coordonner des activités avec les intervenants, ce qui comprend les administrations municipales, lorsqu'il y a lieu, et avec des associations et des propriétaires et des exploitants d'infrastructures essentielles.
Propriétaires et exploitants d'infrastructures essentielles	Gérer ensemble les risques liés à leurs infrastructures essentielles	• Gérer les risques liés à leurs propres infrastructures essentielles • Participer aux activités de recensement des infrastructures essentielles, d'évaluation, de prévention, d'atténuation, de préparation, d'intervention et de rétablissement

Source : *Plan d'action sur les infrastructures essentielles* (2010)

Annexe B :

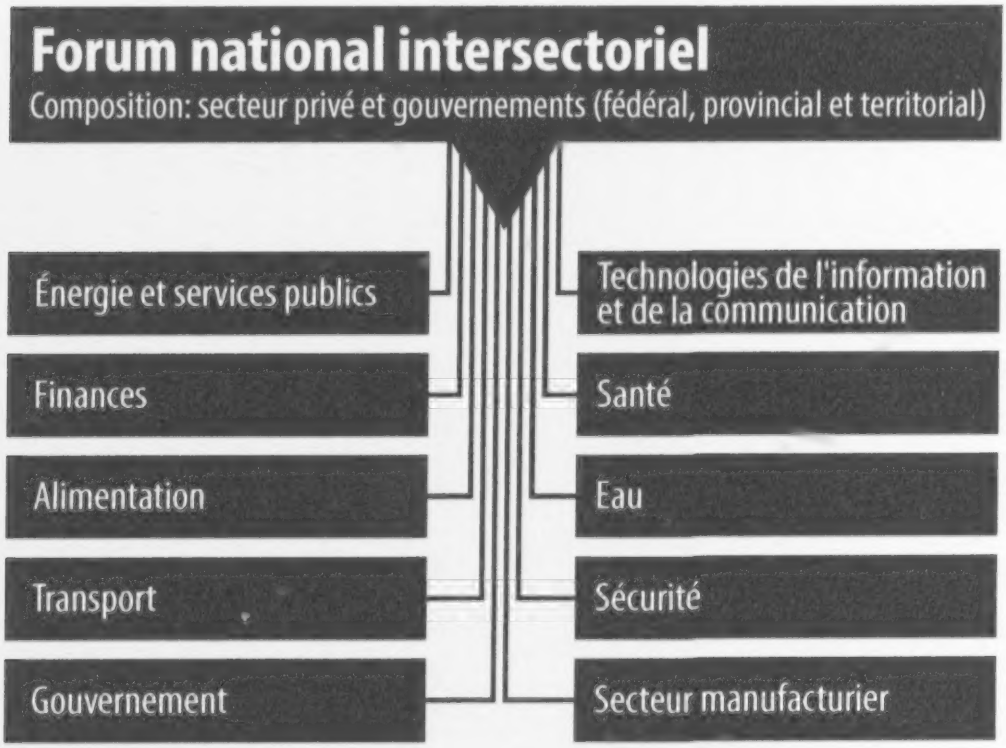
Secteurs des infrastructures essentielles et ministères ou organismes fédéraux responsables

Secteur	Ministères et organismes fédéraux responsables
Énergie et services publics	Ressources naturelles Canada
Technologies de l'information et de la communication	Innovation, Sciences et Développement économique Canada
Finances	Finances Canada
Santé	Agence de la santé publique du Canada
Alimentation	Agriculture et Agroalimentaire Canada
Eau	Environnement et Changement climatique Canada
Transport	Transports Canada
Sécurité	Sécurité publique Canada
Gouvernement	Sécurité publique Canada
Secteur manufacturier	Innovation, Sciences et Développement économique Canada; Ministère de la Défense nationale

Source : *Plan d'action sur les infrastructures essentielles* (2010)

Annexe C :

Réseaux sectoriels et Forum national intersectoriel



Source : *Stratégie nationale sur les infrastructures essentielles* (2010)

Annexe D :

Réalisations dans le cadre du *Plan d'action sur les infrastructures essentielles (2014 - 2017)*

Objectif stratégique

MAINTIEN ET RENFORCEMENT DES PARTENARIATS

Résultats attendus	État actuel
Élaborer un appel à l'action en matière de résilience des infrastructures essentielles	Terminé
Orienter les efforts afin d'assurer une représentation appropriée au sein des réseaux sectoriels	Terminé
Tenir compte des problèmes dans l'ensemble des secteurs lors de réunions multisectorielles	Terminé (et en continu)
Renforcer les communications avec le public et la sensibilisation de la population	Terminé (et en continu)

Objectif stratégique

ÉCHANGER DES RENSEIGNEMENTS ET ASSURER LEUR PROTECTION :

Résultats attendus	État actuel
Accroître le nombre de membres de la Passerelle d'information canadienne sur les infrastructures essentielles et leur participation à celui-ci et tirer parti des capacités de la Passerelle pour améliorer l'échange de renseignements et la collaboration relativement à des projets précis	Terminé (et en continu)
Promouvoir l'obtention d'autorisations de sécurité pour les intervenants du secteur privé afin de permettre l'échange d'information de nature délicate	Terminé (et en continu)
Intensifier l'échange d'information et examiner le processus de rationalisation des dispositions actuelles en matière d'échange d'information	Terminé
Fournir des évaluations des répercussions lors d'événements d'importance nationale	Terminé (et en continu)

Objectif stratégique

MISE EN ŒUVRE D'UNE APPROCHE DE GESTION TOUS RISQUES

Résultats attendus	État actuel
Mettre en œuvre le Programme d'évaluation de la résilience régionale (PERR) partout au Canada	Terminé (et en continu)
Faire une description globale des principaux risques qui pèsent sur les infrastructures essentielles, y compris les dépendances et les tendances en émergence	Terminé (et en continu)

Résultats attendus	État actuel
Évaluer les répercussions d'événements peu probables à forte incidence potentielle sur les secteurs d'infrastructures essentielles afin de mieux connaître et de mieux comprendre les risques qui pèsent sur les infrastructures essentielles	Terminé (et en continu)
Promouvoir l'adoption de normes existantes et déterminer s'il est nécessaire de mettre en place d'autres normes pour renforcer la résilience des infrastructures essentielles	Terminé (et en continu)
Effectuer des exercices visant à renforcer les activités de préparation et d'intervention	Terminé (et en continu)
Créer des produits ciblés en matière d'évaluation des risques pour donner suite à des problèmes en émergence en matière d'infrastructures essentielles	Terminé (et en continu)
Mener à bien le processus d'application nationale d'un modèle relatif aux interdépendances	En continu
Mesurer les progrès accomplis en matière de résilience pour démontrer les résultats et surveiller les progrès	Terminé (et en continu)

Annexe E :
Plan d'action 2018-2020 : Tableau sommaire

CRÉATION ET AMÉLIORATION DE PARTENARIATS

Résultats attendus	Calendrier
Tenir compte des problèmes dans l'ensemble des secteurs lors de réunions multisectorielles	En continu
Collaborer avec les provinces et les territoires afin de renforcer la résilience des infrastructures essentielles	En continu
Collaborer de manière continue avec les ministères fédéraux responsables	En continu
Accroître la portée régionale des programmes des infrastructures essentielles	1re année
Participer à différents forums internationaux pour aborder les questions touchant les infrastructures essentielles	En continu

PARTAGE ET PROTECTION DES RENSEIGNEMENTS

Résultats attendus	Calendrier
Moderniser et promouvoir la Passerelle d'information sur les infrastructures essentielles	En continu
Procéder à une analyse environnementale sur l'échange de renseignements	2e année
Réunir et diffuser des renseignements sur les risques en période de régime stable et au cours d'événements perturbateurs	En continu
Appuyer l'obtention d'attestations de sécurité parmi les intervenants du secteur privé	En continu

MISE EN ŒUVRE D'UNE APPROCHE DE GESTION TOUS RISQUES

Résultats attendus	Calendrier
Accroître l'effet des évaluations de la résilience	2e année
Mettre en œuvre une approche axée sur les risques pour cerner les biens et les infrastructures à caractère important	2e année
Déterminer des moyens pour encourager la communauté des infrastructures essentielles à prendre des mesures afin de réduire les risques	2e année
Tenir des exercices intersectoriels visant à renforcer les activités de préparation et d'intervention	En continu
Évaluer l'état de santé des dix réseaux sectoriels des infrastructures essentielles	En continu
Soutenir la communauté dans la gestion des risques associés à la convergence des systèmes d'infrastructures essentielles physiques et cybernétiques (2010)	En continu
Réviser la *Stratégie nationale pour les infrastructures essentielles* afin de déterminer s'il y a un besoin de mettre à jour l'approche globale du Canada pour la résilience des infrastructures essentielles (2010)	3e année
Concevoir un mécanisme de suivi pour évaluer la progression des activités du *Plan d'action*	En continu

Annexe F :

Ressources

Les sites Web suivants contiennent des informations utiles sur la résilience des infrastructures essentielles au Canada :

***Stratégie nationale sur les infrastructures essentielles* :**
https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-fr.aspx

Sécurité publique Canada/Infrastructures essentielles :
https://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fr.aspx

Passerelle d'information canadienne sur les infrastructures essentielles :
https://cigateway.ps.gc.ca

Gendarmerie royale du Canada (GRC) :
http://www.grc.gc.ca/fr

Service canadien du renseignement de sécurité (SCRS) :
https://csis.gc.ca/index-fr.php

Centre canadien de réponse aux incidents cybernétiques (CCRIC) :
https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-fr.aspx

***Stratégie de cybersécurité du Canada* :**
https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-fr.aspx

***Renforcer la résilience face au terrorisme : Stratégie antiterroriste du Canada* :**
https://www.securitepublique.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/cntr-trrrsm-strtg-fr.aspx

Base de données canadienne sur les catastrophes
https://www.securitepublique.gc.ca/cnt/rsrcs/cndn-dsstr-dtbs/index-fr.aspx

***Rapport des consultations sur l'examen de la cybersécurité* :**
https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/index-fr.aspx

Échange canadien de menaces cybernétiques (ECMC) :
https://cctx.ca/?lang=fr